IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

ASHLEY POPA, individually and on behalf of all others similarly situated, Plaintiff, v. PSP GROUP, LLC d/b/a PET SUPPLIES PLUS and MICROSOFT CORPORATION, Defendants.	Case No. 2:22-cv-1357 **JURY TRIAL DEMANDED**

COMPLAINT - CLASS ACTION

Plaintiff, Ashley Popa ("Plaintiff"), individually and on behalf of all others similarly situated, hereby files this class action complaint against Defendants PSP Group, LLC d/b/a Pet Supplies Plus ("PSP") and Microsoft Corporation ("Microsoft" or collectively with PSP, "Defendants"), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action to combat insidious privacy intrusions resulting from the clandestine deployment of surveillance software on the internet.

2. Specifically, Plaintiff brings this class action against PSP for wiretapping the electronic communications of visitors to its website, www.petsuppliesplus.com, and against Microsoft for wiretapping the electronic communications of visitors across all of Microsoft's clients' websites, including, but not limited to, PSP's website.

3. PSP procures third-party vendors, such as Microsoft, to embed snippets of JavaScript computer code ("Session Replay Code") on PSP's website, which then deploys on each

website visitor's internet browser for the purpose intercepting and recording the website visitor's electronic communications with the PSP website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time ("Website Communications").

4. These third-party vendors, including Microsoft, create and deploy the Session Replay Code at PSP's request (collectively, "Session Replay Providers").

5. After intercepting and capturing the Website Communications, PSP and Session Replay Providers use those Website Communications to recreate website visitors' entire visit to www.petsuppliesplus.com. Session Replay Providers create a video replay of the user's behavior on the website and provide it to PSP for analysis. PSP's procurement of Session Replay Providers, including Microsoft, to secretly deploy Session Replay Codes results in the electronic equivalent of "looking over the shoulder" of each visitor to the PSP website for the entire duration of their website interaction.

6. Microsoft provides its Session Replay Code—Clarity—to a vast number of website clients, including PSP, wiretapping Website Communications from users of each of its client's websites.

7. Defendants' conduct violates the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5701, *et. seq*., and constitutes an invasion of the privacy rights of website visitors.

8. Plaintiff brings this action: 1) individually and on behalf of a class of all Pennsylvania citizens whose Website Communications were intercepted through PSP's procurement and use of Session Replay Code embedded on the webpages of www.petsuppliesplus.com; and 2) individually and on behalf of a class of all Pennsylvania citizens

whose Website Communications were intercepted through Microsoft's Session Replay Code embedded on any of Microsoft's clients' webpages. Plaintiff, on behalf of herself and the classes, seeks all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys' fees and costs.

PARTIES

9. Plaintiff Ashley Popa is a citizen of the Commonwealth of Pennsylvania, and at all times relevant to this action, resided and was domiciled in Lawrence County, Pennsylvania. Plaintiff is a citizen of Pennsylvania.

10. Defendant PSP Group, LLC is corporation organized under the laws of Delaware, and its principal place of business is located at 17197 N. Laurel Park Drive, Suite 402, Livonia, Michigan 48152. Defendant PSP is a citizen of Michigan.

11. Defendant Microsoft is corporation organized under the laws of Washington, and its principal place of business is located in Redmond, Washington. Defendant Microsoft is a citizen of Washington.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed classes, and at least one member of the proposed classes, including Plaintiff, is a citizen of a state different than Defendants.

13. This Court has personal jurisdiction over Defendants because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in Pennsylvania. The privacy violations complained of herein resulted from Defendants' purposeful and tortious acts directed

towards citizens of Pennsylvania. At all relevant times, Defendants knew that its practices would directly result in collection of information from Pennsylvania citizens while those citizens browse webpages with Clarity embedded on it, including www.petsuppliesplus.com. Defendants chose to avail itself of the business opportunities in Pennsylvania and to collect real-time data from website visit sessions initiated by Pennsylvanians, and the claims alleged herein arise from those activities.

14. PSP also knows that many users visit and interact with PSP's website while they are physically present in Pennsylvania. Both desktop and mobile versions of PSP's website allow a user to search for nearby stores by providing the user's "current location," as furnished by the location-determining tools of the device the user is using or by the user's IP address (*i.e.*, without requiring the user to manually input an address). Users' employment of automatic location services in this way means that PSP is continuously made aware that its website is being visited by people located in Pennsylvania, and that such website visitors are being wiretapped in violation of Pennsylvania statutory and common law.

15. Further, Microsoft can also detect a user's location using Clarity. In this way, Microsoft is continuously made aware that its clients' websites are being visited by people located in Pennsylvania, and that such website visitors are being wiretapped in violation of Pennsylvania statutory and common law.

16. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

17. The "world's most valuable resource is no longer oil, but data."[1]

18. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business's website, applications, and emails), behavioral data (*i.e.*, customers' purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.[2] This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.[3]

19. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[4]

20. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of

---

[1] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data.

[2] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, Business News Daily (Aug. 5, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[3] *Id.*

[4] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

Methodologies for Measuring Monetary Value."[5] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[6]

21. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[7]

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites

22. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that "a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected."[8]

23. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.[9] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[10]

---

[5] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.
[6] *Id.* at 25.
[7] *Id.*
[8] Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/.
[9] *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html.
[10] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

24. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

25. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[11]

26. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[12]

27. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[13]

C. How Session Replay Code Works

28. Session Replay Code, such as that implemented on www.petsuppliesplus.com, enables website operators to record, save, and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with

[11] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.
[12] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confusedand-feeling-lack-of-control-over-their-personal-information/.
[13] Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

insights into the user experience by recording website visitors "as they click, scroll, type or navigate across different web pages."[14]

29. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website operator, or has not finished submitting the data to the website operator.[15] As a result, website visitors "aren't just sharing data with the [web]site they're on . . . but also with an analytics service that may be watching over their shoulder."[16]

30. Session Replay Code works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of actions the user takes. When a website delivers Session Replay Code to a user's browser, the browser will follow the code's instructions by sending responses in the form of "event" data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

---

[14] Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/.

[15] *Id.*

[16] Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0.

31. The types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user's navigation and interaction through the website. In order to permit a reconstruction of a user's visit accurately, the Session Replay Code must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

32. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

33. Once the events from a user session have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user's visit through the Session Replay Provider, usually in the form of a video, meaning "[u]nlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions."[17]

34. Because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.[18]

---

[17] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

[18] *Id.*

35. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a "submit" or "enter" button on the website, the Session Replay Code may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

36. Session Replay Code does not necessarily anonymize user sessions, either.

37. First, if a user's entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

38. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

39. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.[19]

40. Session Replay Providers often create "fingerprints" that are unique to a particular user's combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

[19] *Id.*; *see also FS.identify – Identifying users*, FullStory, https://help.fullstory.com/hc/en-us/articles/360020828113, (last visited Sep. 22, 2022).

41. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user's other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

42. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.[20] Indeed, "[t]he more copies of sensitive information that exist, the broader the attack surface, and when data is being collected [ ] it may not be stored properly or have standard protections" increasing "the overall risk that data will someday publicly leak or be breached."[21]

43. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.[22] In announcing this decision, Apple stated: "Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity."[23]

---

[20] Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720.

[21] Lily Hay Newman, *Covert 'Replay Sessions' Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/.

[22] Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), https://techcrunch.com/2019/02/07/apple-glassbox-apps/.

[23] *Id.*

D. PSP Secretly Wiretaps its Website Visitors' Electronic Communications

44. PSP operates the website www.petsuppliesplus.com. PSP offers pet-related products through its website such as dog beds, cat toys, fish food, and the like.

45. However, unbeknownst to the millions of individuals perusing PSP's products online, PSP intentionally procures and embeds various Session Replay Codes from Session Replay Providers on its website to track and analyze website user interactions with www.petsuppliesplus.com.

46. One such Session Replay Provider that PSP procures is Microsoft.

47. Microsoft is the owner and operator of a Session Replay Code titled Clarity, which provides basic information about website user sessions, interactions, and engagement, and breaks down users by device type, country, and other dimensions.[24]

48. PSP's procurement and use of Microsoft Clarity's Session Replay Code, and procurement and use of other Session Replay Codes through various Session Replay Providers, is a wiretap in violation of Pennsylvania statutory and common law.

E. Microsoft Secretly Wiretaps its Clients' Website Visitors' Electronic Communications

49. Clarity captures a user's interactions with a website, logging every website user's mouse movements and clicks, scrolling window resizing, user inputs, and more.[25] Indeed, Clarity organizes the information it captures into over 30 different categories including: the date a user visited the website, the device the user accessed the website on, the type of browser the user accessed the website on, the operating system of the device used to access the website, the country

[24] Jono Alderson, *An Introduction to Microsoft Clarity*, Yoast, https://yoast.com/introduction-microsoft-clarity/#h-what-is-microsoft-clarity, (last visited Sep. 22, 2022).
[25] *Clarity Data Collection*, Microsoft, https://docs.microsoft.com/en-us/clarity/clarity-data, (last visited Sep. 22, 2022).

where the user accessed the website from, a user's mouse movements, a user's screen swipes, text inputted by the user on the website, and how far down a webpage a user scrolls.[26] Clarity even provides a specific user ID to each website visitor so their website use and interactions can be monitored over time. [27]

50. Similar to other Session Replay Code, the information collected and recorded by Clarity can then be used to play back a user's journey through a website, showing how they interacted with site navigation, calls to action, search features, and other on-page elements.[28] Put differently, the information Clarity captures can be translated into a simulation video of how a user interacts with a website.

51. Clarity also uses the information captured to create detailed heatmaps of a website that provide information about which elements of a website have high user engagement, how far website users scrolled on the website, and the total clicks within a given area on the website. [29]

52. As such, Clarity collects highly personal information and substantive communications that can be tied directly to a website user's identity as it monitors, records, and collects a website user's every move.

53. Clarity offers websites three standard approaches when it comes to masking sensitive information collected from a user's interactions with a website—strict (all text entered by a user is purportedly masked), balanced (sensitive text entered into certain specifically pre-coded fields, such as passwords, and credit card information, is masked), and relaxed (no text

---

[26] *Filters Overview*, Microsoft (Jul. 26, 2022), https://docs.microsoft.com/en-us/clarity/clarity-filters.
[27] *Id.*
[28] Roger Montti, *Microsoft Clarity Analytics: Everything You Need to Know*, SEJ (Jan. 19, 2022), https://www.searchenginejournal.com/microsoft-clarity-analytics-overview/419311/#close.
[29] Haley Walden, *What is Microsoft Clarity? (& How Can it Improve SEO?)*, Elegant Themes (Jun. 12, 2022), https://www.elegantthemes.com/blog/wordpress/microsoft-clarity-improve-seo.

entered by a user is masked).[30] When Clarity is set to "relaxed," whatever information a user enters into the field on a website can be previewed in session recordings.[31] Additionally, Clarity enables websites to select specific elements and content to mask or unmask, customizing the standard masking approaches. [32]

54. However, even when a website operator selects the "strict" and "balanced" settings, Clarity is nevertheless capable of collecting text entered by users, including text containing sensitive information.

55. In order for Clarity to capture website visitors' interactions with a website, Clarity's JavaScript must be installed on the website, either directly hard-coded on the website or on a third-party platform, such as Google Tag Manager.[33] Clarity is embedded in a website by adding its JavaScript code into the HyperText Markup Language (HTML) underlying the website. As with all HTML code, Clarity is not visible to a user who is navigating a webpage through a standard browser's default view, because by design a browser will interpret HTML, without showing it, in order to render a more user-friendly display that is the designer's intended presentation of the website to a visitor.

56. Clarity can be revealed to technical users who understand web technologies and can enable alternative display modes that will show underlying HTML, such as "developer tools," but even then, the users would first need to know what they are looking for in order to find the

[30] *Microsoft Clarity, An Essential Part of Customer Experience Optimization*, TechAir (Aug. 17, 2022), https://privacy.microsoft.com/en-US/privacystatement.
[31] *Id.*
[32] *Masking Content*, Microsoft (Jul. 18, 2022), https://docs.microsoft.com/en-us/clarity/clarity-masking.
[33] *Set Up Clarity*, Microsoft (Jul. 18, 2022), https://docs.microsoft.com/en-us/clarity/clarity-setup.

script. Developer tools are intended for website programmers and are generally not meaningful or comprehensible by those without a background in computer science.

57. Once Clarity's JavaScript is installed on a website, Clarity begins collecting website user's interactions within two hours of installation.[34] Once deployed, the wiretapping commences immediately on the visitor's web browser when the visitor loads a website in their browser.

58. Data collected by Clarity is then stored in the Microsoft Aure cloud service, and Microsoft has access to that information. [35]

F. Plaintiff's and Class Members' Experience

59. Plaintiff has visited www.petsuppliesplus.com on her computer while in Pennsylvania.

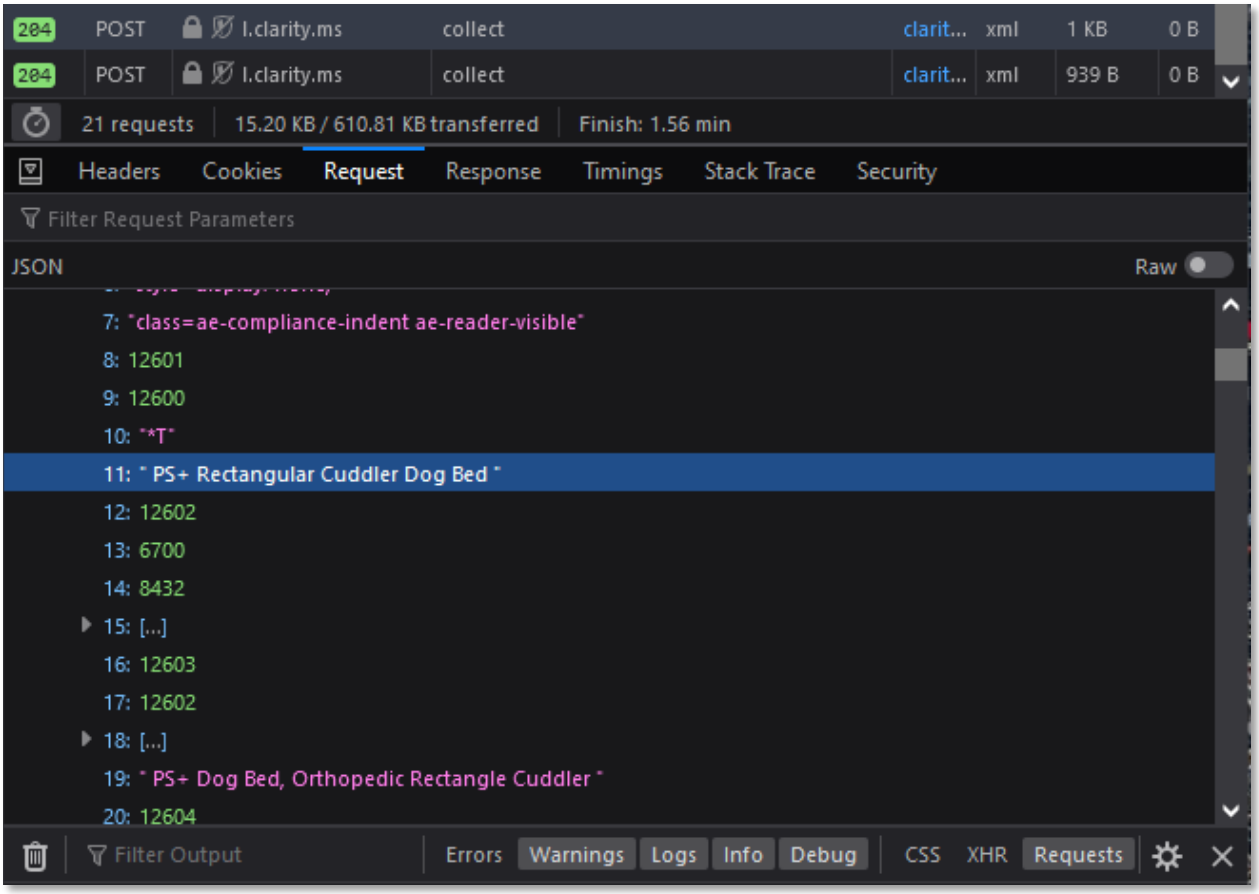
60. While visiting PSP's website, Plaintiff fell victim to Defendants' unlawful monitoring, recording, and collection of Plaintiff's Website Communications with www.petsuppliesplus.com.

61. Unknown to Plaintiff, PSP procures and embeds Microsoft Clarity on its website.

62. During the website visit, Plaintiff's Website Communications were captured by Microsoft Clarity and sent to Microsoft.

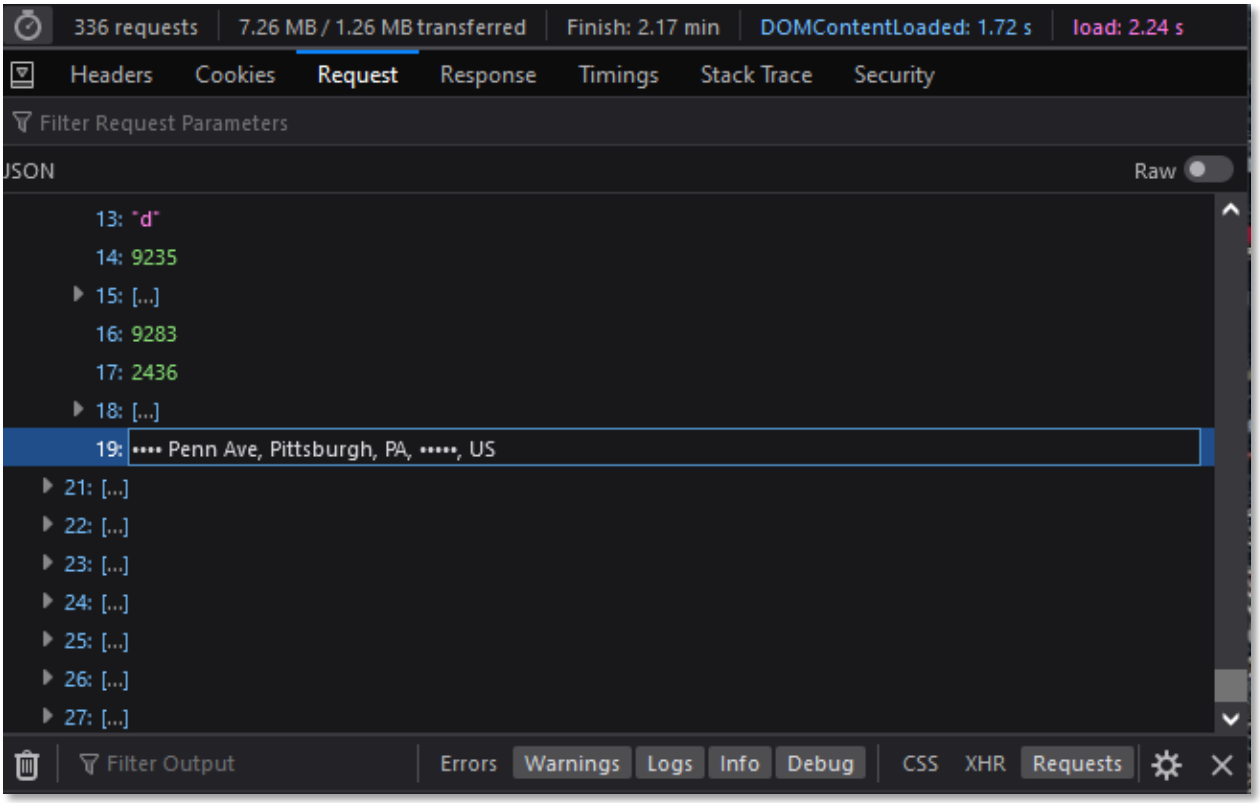
63. For example, when visiting www.petsuppliesplus.com, if a website user views a certain product offered for sale, that information is captured by Microsoft Clarity embedded on the website:

[34] *Frequently Asked Questions*, Microsoft, https://docs.microsoft.com/en-us/clarity/faq, (last visited Aug. 24, 2022).
[35] *Id.*



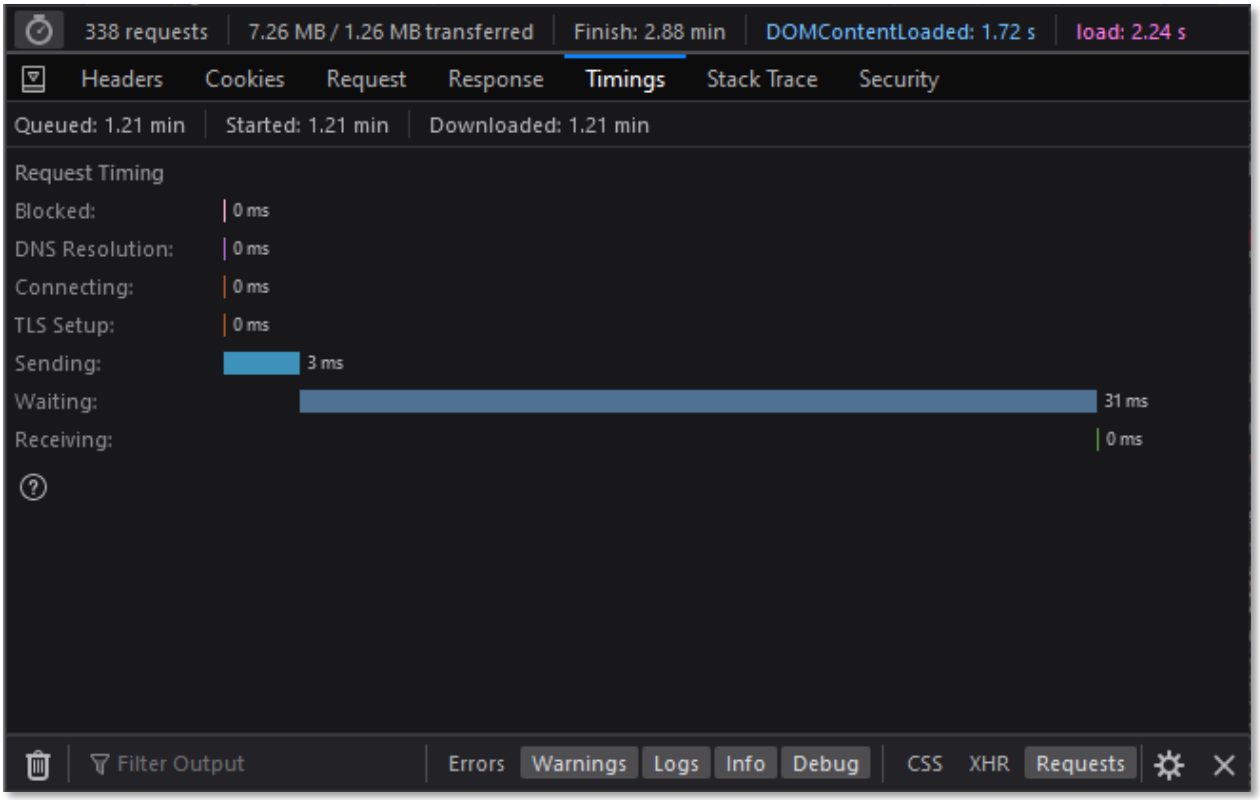
Depicting information sent to one of the Session Replay Providers—Microsoft—through a Session Replay Code—Clarity—after viewing the "Rectangular Cuddler Bed" while visiting www.petsuppliesplus.com.

64. Similarly, when visiting www.petsuppliesplus.com, if a user enters their address for delivery, that information is captured by Microsoft Clarity embedded on the website:



Depicting information sent to one of the Session Replay Providers—Microsoft—through a Session Replay Code—Clarity—after entering an address to a text box.

65. The wiretapping by Session Replay Providers area ongoing during the visit and intercepts the contents of these communications between Plaintiff and PSP with instantaneous transmissions to Session Replay Providers. As illustrated below, it took only 34 milliseconds to send a packet of event response data to Microsoft, which would indicate whatever the website user had just done:



66. The Session Replay Codes on PSP's website operate in the same manner for all putative PSP Class members.

67. Like Plaintiff, each PSP Class member visited www.petsuppliesplus.com with Session Replay Code embedded in it, and those Session Replay Codes intercepted the PSP Class members' Website Communications with www.petsuppliesplus.com by sending hyper-frequent logs of those communications to Session Replay Providers.

68. Microsoft Clarity operates in a similar manner across all of its clients' websites.

69. Like Plaintiff, each Microsoft Class member visited a website with Clarity embedded in it, and Clarity intercepted the Microsoft Class members' Website Communications by sending hyper-frequent logs of those communications to Microsoft.

70. Even if websites mask certain elements when they configure the settings of the Session Replay Code embedded on their website, any operational iteration of the Session Replay

Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

71. For example, even with heightened masking enabled, Session Replay Providers like Microsoft will still learn through the intercepted data exactly which pages a user navigates to, how the user moves through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

72. As a specific example, if a user types a particular product into PSP's search bar, even if the text entered into the search bar is masked, Session Replay Providers will still learn what is entered into the bar as soon as the search result page loads. This is so because the responsive search results will be displayed on the subsequent page, and the responsive content generated by PSP will repeat the searched information back on the generated page. That information will not be masked even if user-inputted text is fully masked in a text field.

CLASS ACTION ALLEGATIONS

73. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Classes:

Microsoft Class:

All natural persons in Pennsylvania whose Website Communications emanating from Pennsylvania were captured through the use of Microsoft Clarity.

PSP Class:

All natural persons in Pennsylvania whose Website Communications emanating from Pennsylvania were captured through the use of Session Replay Code embedded in www.petsuppliesplus.com.

74. Excluded from the Classes are Defendants, their parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Classes,

the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

75. **Numerosity:** The members of the Classes are so numerous that individual joinder of all Class members is impracticable. The precise number of Class members and their identities may be obtained from the books and records of PSP or the Session Replay Providers.

76. **Commonality:** This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to: (a) whether Defendant PSP procures Session Replay Providers to intercept PSP's website visitors' Website Communications; (b) whether Defendant Microsoft acquired the contents of website users' Website Communications without their consent; (c) whether PSP intentionally discloses the intercepted Website Communications of its website users; (d) whether Defendants acquire the contents of website users' Website Communications without their consent; (e) whether Defendants' conduct violates Pennsylvania Wiretap Act,18 Pa. Cons. Stat. § 5701, *et seq*.; (f) whether Defendants invaded website users' privacy by intercepting their Website Communications; (g) whether Plaintiff and the Class members are entitled to equitable relief; and (h) whether Plaintiff and the Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

77. **Typicality:** Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiff and each member of the Classes had their communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiff and the members of the Classes typical of one another.

78. **Adequacy of Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Classes. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Classes, and Defendants have no defenses unique to Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and they have the resources to do so. Neither Plaintiff nor her counsel have any interest adverse to the interests of the other members of the Classes.

79. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Classes are impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

80. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Classes. If Defendants intercepted Plaintiff's and Class members' Website Communications, then Plaintiff and each Class member suffered damages by that conduct.

81. **Ascertainability:** Members of the Classes are ascertainable. Class membership is defined using objective criteria, and Class members may be readily identified through PSP's books and records or the Session Replay Providers' books and records.

COUNT I
Violation of Pennsylvania Wiretap Act
18 Pa. Cons. Stat. § 5701, et. Seq.
(against Microsoft)

82. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

83. Plaintiff brings this claim individually and on behalf of the Microsoft Class.

84. The Pennsylvania Wiretap Act (the "Act") prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

85. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

86. "Intercept" is defined as any "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. Cons. Stat. § 5702.

87. "Contents" is defined as "used with respect to any wire, electronic or oral communication, is any information concerning the substance, purport, or meaning of that communication." 18 Pa. Cons. Stat. § 5702.

88. "Person" is defined as "any individual, partnership, association, joint stock company, trust or corporation." 18 Pa. Cons. Stat. § 5702.

89. "Electronic Communication" is defined as "[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." 18 Pa. Cons. Stat. § 5702.

90. Microsoft is a person for purposes of the Act because it is a corporation.

91. Session Replay Code like Microsoft's Clarity is a "device" used for the "acquisition of the contents of any wire, electronic, or oral communication" within the meaning of the Act.

92. Plaintiff's and Microsoft Class members' intercepted Website Communications constitute the "contents" of electronic communication[s]" within the meaning of the Act.

93. Plaintiff's and Microsoft Class members' electronic communications are intercepted contemporaneously with their transmission.

94. Plaintiff and Microsoft Class members did not consent to having their Website Communications wiretapped.

95. Microsoft intentionally intercepted or endeavored to intercept Plaintiff's and Microsoft Class members' Website Communications; intentionally disclosed or endeavored to disclose the contents of Plaintiff's and Microsoft Class members' Website Communications obtained through a wiretap; and/or intentionally used or endeavored to use the contents of Plaintiff's and Microsoft Class members' Website Communications obtained through a wiretap.

96. Pursuant to 18 Pa. Cons. Stat. 5725(a), Plaintiff and the Microsoft Class members seek (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

97. Microsoft's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Microsoft Class members any time they visit a website with Microsoft Clarity enabled without their consent. Plaintiff and Microsoft Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT II
Violation of Pennsylvania Wiretap Act
18 Pa. Cons. Stat. § 5701, et. seq.
(against PSP)

98. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

99. Plaintiff brings this claim individually and on behalf of the PSP Class.

100. The Pennsylvania Wiretap Act (the "Act") prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

101. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the

rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

102. "Intercept" is defined as any "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. Cons. Stat. § 5702.

103. "Contents" is defined as "used with respect to any wire, electronic or oral communication, is any information concerning the substance, purport, or meaning of that communication." 18 Pa. Cons. Stat. § 5702.

104. "Person" is defined as "any individual, partnership, association, joint stock company, trust or corporation." 18 Pa. Cons. Stat. § 5702.

105. "Electronic Communication" is defined as "[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." 18 Pa. Cons. Stat. § 5702.

106. PSP is a person for purposes of the Act because it is a corporation.

107. Session Replay Code like that procured by PSP is a "device" used for the "acquisition of the contents of any wire, electronic, or oral communication" within the meaning of the Act.

108. Plaintiff's and PSP Class members' intercepted Website Communications constitute the "contents" of electronic communication[s]" within the meaning of the Act.

109. PSP intentionally procures and embeds Session Replay Code on its website to spy on, automatically and secretly, and intercept its website visitors' electronic interactions communications with PSP in real time.

110. Plaintiff's and PSP Class members' electronic communications are intercepted contemporaneously with their transmission.

111. Plaintiff and PSP Class members did not consent to having their Website Communications wiretapped.

112. Pursuant to 18 Pa. Cons. Stat. 5725(a), Plaintiff and the PSP Class members seek (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

113. PSP's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and PSP Class members any time they visit PSP's website with Session Replay Code enabled without their consent. Plaintiff and PSP Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT III
Invasion of Privacy – Intrusion Upon Seclusion
(against Microsoft)

114. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

115. Plaintiff brings this claim individually and on behalf of the Microsoft Class.

116. Pennsylvania common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in multiple sections of the Pennsylvania constitution.

117. Plaintiff and Microsoft Class members have an objective, reasonable expectation of privacy in their Website Communications.

118. Plaintiff and Microsoft Class members did not consent to, authorize, or know about Microsoft's intrusion at the time it occurred. Plaintiff and Microsoft Class members never agreed that Microsoft could collect or disclose their Website Communications.

119. Plaintiff and Microsoft Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

120. Microsoft intentionally intrudes on Plaintiff's and Microsoft Class members' private life, seclusion, or solitude, without consent.

121. Microsoft's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

122. Plaintiff and Microsoft Class members were harmed by Microsoft's wrongful conduct as Microsoft's conduct has caused Plaintiff and the Microsoft Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

123. Microsoft's conduct has needlessly harmed Plaintiff and the Microsoft Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Microsoft Class to experience mental anguish, emotional distress, worry, fear, and other harms.

124. Additionally, given the monetary value of individual personal information, Microsoft deprived Plaintiff and Microsoft Class members of the economic value of their interactions with Microsoft's clients' website, without providing proper consideration for Plaintiff's and Microsoft Class members' property.

125. Further, Microsoft has improperly profited from its invasion of Plaintiff's and Microsoft Class members' privacy in its use of their data for its economic value.

126. As a direct and proximate result Microsoft's conduct, Plaintiff and Microsoft Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

127. Microsoft's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Microsoft Class members any time they visit Microsoft's clients' website with Clarity enabled without their consent. Plaintiff and Microsoft Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT IV
Invasion of Privacy – Intrusion Upon Seclusion
(against PSP)

128. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

129. Plaintiff brings this claim individually and on behalf of the PSP Class.

130. Pennsylvania common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in multiple sections of the Pennsylvania constitution.

131. Plaintiff and PSP Class members have an objective, reasonable expectation of privacy in their Website Communications.

132. Plaintiff and PSP Class members did not consent to, authorize, or know about PSP's intrusion at the time it occurred. Plaintiff and PSP Class members never agreed that PSP could collect or disclose their Website Communications.

133. Plaintiff and PSP Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

134. PSP intentionally intrudes on Plaintiff's and PSP Class members' private life, seclusion, or solitude, without consent.

135. PSP's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

136. Plaintiff and PSP Class members were harmed by PSP's wrongful conduct as PSP's conduct has caused Plaintiff and the PSP Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

137. PSP's conduct has needlessly harmed Plaintiff and the PSP Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the PSP Class to experience mental anguish, emotional distress, worry, fear, and other harms.

138. Additionally, given the monetary value of individual personal information, PSP deprived Plaintiff and PSP Class members of the economic value of their interactions with PSP's website, without providing proper consideration for Plaintiff's and PSP Class members' property.

139. Further, PSP has improperly profited from its invasion of Plaintiff's and PSP Class members' privacy in its use of their data for its economic value.

140. As a direct and proximate result PSP's conduct, Plaintiff and PSP Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

141. PSP's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and PSP Class members any time they visit PSP's website with Session Replay Code enabled without their consent. Plaintiff and PSP Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other members of the proposed Classes, respectfully request that the Court enter judgment in Plaintiff's and the Class's favor and against Defendants as follows:

A. Certifying the Classes and appointing Plaintiff as Class representative;

B. Appointing Plaintiff's counsel as class counsel;

C. Declaring that Defendants' past conduct was unlawful, as alleged herein;

D. Declaring Defendants' ongoing conduct is unlawful, as alleged herein;

E. Enjoining Defendants from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Classes, demands a trial by jury of any and all issues in this action so triable of right.

Dated: September 22, 2022

Respectfully submitted,

/s/ Gary F. Lynch
Gary F. Lynch
Kelly K. Iverson
Jamisen A. Etzel
Elizabeth Pollock-Avery
Nicholas A. Colella
Patrick D. Donathen
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Telephone: 412-322-9243
Facsimile: 412-231-0246
gary@lcllp.com
kelly@lcllp.com
jamisen@lcllp.com
elizabeth@lcllp.com
nickc@lcllp.com
patrick@lcllp.com

Attorneys for Plaintiff and the proposed Classes